

Survey : the trend of the Web-based Browser Fingerprinting in the last 5 years

Hyunjoo Lee
sn220865@kaist.ac.kr

ACM Reference Format:

Hyunjoo Lee. 2019. Survey : the trend of the Web-based Browser Fingerprinting in the last 5 years. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 INTRODUCTION

In 2010, Eckerlsey [?] introduced browser fingerprinting which is stateless tracking technique. When users visit some browser, their device provides the information of the site they visited including a set of browser and system attributes such as operating system, settings, and the hardware details. The combination of this information is called browser fingerprinting, and it can be used to identify and track users. In 2018, Vastel [?] introduced 4 distinct levels in which fingerprint inconsistencies are detected; OS-level, browser-level, device-level, and canvas-level. From this paper, we found that we can obtain the features of browser fingerprints from those four different levels. Based on this idea, we will implement various fingerprinters by using attributes divided into 4 distinct levels, and evaluate which level and which attributes are more efficient to identify users. In addition to evaluate general attributes of browser fingerprints, we also implement several fingerprinting technologies only for mobile devices recently discovered[?].

2 UNDERSTANDING FINGERPRINTING

In 2010, Eckerlsey [?] introduced browser fingerprinting which is stateless tracking

2.1 Identify the users with browser-based fingerprinting

Browser fingerprinting is

2.2 Tracking by using the fingerprint

Browser fingerprinting is

3 ANALYSIS OF FINGERPRINTING

3.1 client-side

This section will be written as following steps:

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Conference'17, July 2017, Washington, DC, USA
© 2019 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00
<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

Overall fingerprinting attributes. : "Host Fingerprinting and Traking web" literatures[?????].

Overall mobile and desktop fingerprinting attributes. : "Beauty and the Beast"

Browser extension fingerprinting. : "XHOUND"

Effectiveness in Large scale. : "Hiding in the Crowd" In 2010, Eckersley[?]

Open problems. open problems in here

3.2 server-side

by Vastel *et al.* [?]. This section will be written as following steps:

Fingerprinting Ecosystem. : "Cookieless-Monster"

Diversity of tracking techniques. : "FP-Detective, The Web Never Forgets, Online tracking"

Open problems. open problems in here

4 ADVANCED TECHNIQUES

4.1 Uniqueness

In these days, mobile devices are becoming the main platform for browsing the web. Thus, many studies[????] which found new fingerprints from a mobile device with not only general fingerprinting attributes but also other factors to identify the user have emerged. In this section, we will introduce several fingerprinting attributes.

Cross browser fingerprinting. I"(Cross-) Browser fingerprinting via OS and Hardware Level"

Fingerprint Inconsistencies. "FP-Scanner" volume[?].

Open problems. open problems in here

4.2 Linkability

In these days, mobile devices are becoming the main platform for browsing the web.

5 LINKABILITY

"FP-Stalker"

1) We collect the dataset from the web browser based on the previous literatures[????].

Open problems. open problems in here

6 DEFENSE TECHNIQUES

Block fingerprinter. "PriVaricator(linkability)"

Blocking Tracker. "Block me if you can"

Open problems. open problems in here

7 GDPR'S WEB PRIVACY POLICY ON WEB SERVER

GDPR clausis related in fingerprinting. introduce some statements related in fingerprinting in this part

Evaluation of policy if they are well adopted in real-world.
In real-world case in here

Open problems. open problems in here "We Value Your Privacy"

8 CONCLUSION

This paper will indicate that which level and which attributes are the most efficient one that can identify user well. Also, we will focus on the mobile fingerprinting with diverse factors. Hence, we can indicate that which factor of the mobile fingerprinting attributes considering the-state-of-the-art technologies is the most efficient one on the mobile device. From this paper, we can evaluate the-state-of-the-art techniques compared to previous evaluated technologies.